US PATENT & TRADEMARK OFFICE

PATENT APPLICATION FULL TEXT AND IMAGE DATABASE

Help Home Boolean Manual Number PTDLs

Hit List Bottom

View Shopping Cart Add to Shopping Cart

Images

(1 of 1)

United States Patent Application	***20020144129***
Kind Code	**A1**
Malivanchuk, Taras ; et al.	**October 3, 2002**

System and method for restoring computer systems damaged by a malicious computer program

Abstract

A method for restoring a computer system modified by malicious code. The method scans the computer system for the malicious code, identifies the malicious code and retrieves from a data file, information relating to the malicious code including at least one command used for restoring the computer system to a state that existed prior to modification by the malicious code. The at least one command is executed to restore the computer system to substantially the state as it existed prior to modification by the malicious code.

Inventors: **Malivanchuk, Taras**; *(Holon, IL)* ; **Darzi, Moshe**; *(Petach Tikva, IL)* ; **Rotschield, Ofer**; *(Kiryat Uno, IL)*

Correspondence Name and Address:
RICHARD F. JAWORSKI
Cooper & Dunham LLP
1185 Avenue of the Americas
New York
NY
10036
US

Serial No.:	**823673**
Series Code:	**09**
Filed:	**March 30, 2001**

U.S. Current Class:	**713/188**
U.S. Class at Publication:	**713/188**
Intern'l Class:	H04L 009/32

Claims

What is claimed is:

1. A method for restoring a computer system modified by malicious code, comprising: scanning the computer system for the malicious code; identifying the malicious code; retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system to a state that existed prior to modification by the malicious code; and executing the at least one command to restore the computer system to substantially the state as it existed prior to modification by the malicious code.

2. The method of claim 1, wherein the step of executing the at least one command includes one of reading, writing, and deleting data.

3. The method of claim 1, wherein the step of executing the at least one command includes at least one of renaming and deleting a file.

4. The method of claim 1, wherein the malicious code modifies at least one file and said method comprises: reading from the modified file, a name of a second file; and modifying the second file.

5. The method of claim 1, wherein the data file comprises a plurality of data files, each data file being provided for a particular type of malicious code, each data file including at least one command that can be used for restoring the computer system to a state that existed prior to modification by the particular type of malicious code.

6. A storage medium including computer executable code for restoring a computer system modified by malicious code, comprising: code for scanning the computer system for the malicious code; code for identifying the malicious code; code for retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system to a state that existed prior to modification by the malicious code; and code for executing the at least one command to restore the computer system to substantially the state as it existed prior to modification by the malicious code.

7. The storage medium of claim 6, wherein the code for executing the at least one command includes code for performing at least one one of reading, writing, and deleting data.

8. The storage medium of claim 6, wherein the code for executing the at least one command includes code for performing at least one of renaming and deleting a file.

9. The storage medium of claim 6, wherein the malicious code modifies at least one file, said storage medium further comprising: code for reading from the modified file, a name of a second file; and code for modifying the second file.

10. The storage medium of claim 6, wherein the data file comprises a plurality of data files, each data file being provided for a particular type of malicious code, each data file including at least one command that can be used for restoring the computer system to a state that existed prior to modification by the particular type of malicious code.

11. A computer data signal embodied in a transmission medium and including computer executable

instructions for restoring a computer system modified by malicious code, comprising: a data signal portion for scanning the computer system for the malicious code; a data signal portion for identifying the malicious code; a data signal portion for retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system to a state that existed prior to modification by the malicious code; and a data signal portion for executing the at least one command to restore the computer system to substantially the state as it existed prior to modification by the malicious code.

12. The computer data signal of claim 11, wherein the data signal portion for executing the at least one command performs at least one of reading, writing, and deleting data.

13. The computer data signal of claim 11, wherein the data signal portion for executing the at least one command performs at least one of renaming and deleting a file.

14. The computer data signal of claim 11, wherein the malicious code modifies at least one file, said computer data signal further comprising: a data signal portion for reading from the modified file, a name of a second file; and a data signal portion for modifying the second file.

15. The computer data signal of claim 11, wherein the data file comprises a plurality of data files, each data file being provided for a particular type of malicious code, each data file including at least one command that can be used for restoring the computer system to a state that existed prior to modification by the particular type of malicious code.

16. A programmed computer system including a program for restoring a computer system modified by malicious code, comprising: means for scanning the computer system for the malicious code; means for identifying the malicious code; means for retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system to a state that existed prior to modification by the malicious code; and means for executing the at least one command to restore the computer system to substantially the state as it existed prior to modification by the malicious code.

17. The programmed computer system of claim 16, wherein the means for executing the at least one command includes means for performing at least one of reading, writing, and deleting data.

18. The programmed computer system of claim 16, wherein the means for executing the at least one command includes means for performing at least one of renaming and deleting a file.

19. The programmed computer system of claim 16, wherein the malicious code modifies at least one file and said system further comprises: means for reading from the modified file, a name of a second file; and means for modifying the second file.

20. The programmed computer system of claim 16, wherein the data file comprises a plurality of data files, each data file being provided for a particular type of malicious code, each data file including at least one command that can be used for restoring the computer system to a state that existed prior to modification by the particular type of malicious code.

Description

BACKGROUND

US PATENT & TRADEMARK OFFICE
PATENT APPLICATION FULL TEXT AND IMAGE DATABASE

Help Home Boolean Manual Number PTDLs

Hit List Bottom

View Shopping Cart Add to Shopping Cart

Images

(1 of 1)

United States Patent Application	***20030217286***
Kind Code	**A1**
Carmona, Itshak ; et al.	**November 20, 2003**

System and method for detecting malicious code

Abstract

A method of detecting malicious code in computer readable code includes performing an initial determination to determine whether a first portion of the computer readable code may potentially have malicious code and if it is determined that the computer readable code potentially has malicious code, performing another determination to determine whether a second portion not including the first portion of the computer readable code has malicious code.

Inventors: **Carmona, Itshak**; *(US)* ; **Malivanchuk, Taras**; *(US)*

Correspondence Name and Address:
RICHARD F. JAWORSKI
Cooper & Dunham LLP
1185 Avenue of the Americas
New York
NY
10036
US

Serial No.:	**410974**
Series Code:	**10**
Filed:	**April 10, 2003**

U.S. Current Class:	**713/200**
U.S. Class at Publication:	**713/200**
Intern'l Class:	H04L 009/00

Claims

What is claimed is:

1. A method of detecting malicious code in computer readable code, comprising: performing an initial determination to determine whether a first portion of the computer readable code may potentially have malicious code; and if it is determined that the computer readable code potentially has malicious code, performing another determination to determine whether a second portion not including the first portion of the computer readable code has malicious code.

2. A method as recited in claim 1, wherein the another determination is more comprehensive than the initial determination.

3. A method as recited in claim 1, wherein the initial determination determines a first CRC or the first portion of the computer readable code.

4. A method as recited in claim 3, wherein the another determination is performed to determine a second CRC of the second portion of the computer readable code.

5. A method as recited in claim 4, wherein the first CRC is compared with a database of CRCs to determine whether malicious code is present.

6. A method as recited in claim 5, wherein the second CRC is compared with a CRC in the database.

7. A method as recited in claim 6, wherein the database of CRCs comprises sets of CRCs.

8. A method as recited in claim 7, wherein the sets of CRCs comprise a first viral CRC obtained by determining a CRC of the first portion of the computer readable code modified to include malicious code and a corresponding second viral CRC obtained by determining a CRC of the second portion of the computer readable code modified to include the malicious code.

9. A method of detecting malicious code in computer readable code, comprising: determining a CRC of a first portion of the computer readable code; performing an initial determination to determine whether the CRC of the first portion of the computer readable code is present in a database of CRCs, each CRC including corresponding instructions for how to proceed if the determined CRC is present in the database of CRCs; and if it is determined that the CRC of the first portion of the computer readable code is present in the database of CRCs, performing the corresponding instructions.

10. A method as recited in claim 9, wherein the corresponding instructions comprise at least one of directing that a CRC of the entire computer readable code be determined and compared with the database of CRCs, directing that a CRC of a constant portion of the computer readable code be determined and compared with the database of CRCs, directing that a form of malicious code detection other than CRC checks be performed on the computer readable code.

11 A recording medium including executable code for detecting malicious code in computer readable code, comprising: code for performing an initial determination to determine whether a first portion of the computer readable code may potentially have malicious code; and code for, if it is determined that the computer readable code potentially has malicious code, performing another determination to determine whether a second portion not including the first portion of the computer readable code has malicious code.

12. A recording medium as recited in claim 11, wherein the another determination is more comprehensive than the initial determination.

13. A recording medium as recited in claim 11, wherein the initial determination determines a first CRC of the first portion of the computer readable code.

14. A recording medium as recited in claim 13, wherein the another determination is performed to determine a second CRC of the second portion of the computer readable code.

15. A recording medium as recited in claim 14, wherein the first CRC is compared with a database of CRCs to determine whether malicious code is present.

16. A recording medium as recited in claim 15, wherein the second CRC is compared with a CRC in the database.

17. A recording medium as recited in claim 16, wherein the database of CRCs comprises sets of CRCs.

18. A recording medium as recited in claim 17, wherein the sets of CRCs comprise a first viral CRC obtained by determining a CRC of the first portion of the computer readable code modified to include malicious code and a corresponding second viral CRC obtained by determining a CRC of the second portion of the computer readable code modified to include the malicious code.

19. A recording medium including executable code for detecting malicious code in computer readable code, comprising: code for determining a CRC of a first portion of the computer readable code; code for performing an initial determination to determine whether the CRC of the first portion of the computer readable code is present in a database of CRCs, each CRC including corresponding instructions for how to proceed if the determined CRC is present in the database of CRCs; and code for, if it is determined that the CRC of the first portion of the computer readable code is present in the database of CRCs, performing the corresponding instructions.

20. A recording medium as recited in claim 19, wherein the corresponding instructions comprise at least one of directing that a CRC of the entire computer readable code be determined and compared with the database of CRCs, directing that a CRC of a constant portion of the computer readable code be determined and compared with the database of CRCs, directing that a form of malicious code detection other than CRC checks be performed on the computer readable code.

21. A programmed computer apparatus including code for detecting malicious code in computer readable code, the apparatus capable of performing a method comprising: performing an initial determination to determine whether a first portion of the computer readable code may potentially have malicious code; and if it is determined that the computer readable code potentially has malicious code, performing another determination to determine whether a second portion not including the first portion of the computer readable code has malicious code.

22. A programmed computer apparatus as recited in claim 21, wherein the another determination is more comprehensive than the initial determination.

23. A programmed computer apparatus as recited in claim 21, wherein the initial determination determines a first CRC of the first portion of the computer readable code.

24. A programmed computer apparatus as recited in claim 23, wherein the another determination is

performed to determine a second CRC of the second portion of the computer readable code.

25. A programmed computer apparatus as recited in claim 24, wherein the first CRC is compared with a database of CRCs to determine whether malicious code is present.

26. A programmed computer apparatus as recited in claim 25, wherein the second CRC is compared with a CRC in the database.

27. A programmed computer apparatus as recited in claim 26, wherein the database of CRCs comprises sets of CRCs.

28. A programmed computer apparatus as recited in claim 27, wherein the sets of CRCs comprise a first viral CRC obtained by determining a CRC of the first portion of the computer readable code modified to include malicious code and a corresponding second viral CRC obtained by determining a CRC of the second portion of the computer readable code modified to include the malicious code.

29. A programmed computer apparatus including code for detecting malicious code in computer readable code, the apparatus capable of performing a method comprising: determining a CRC of a first portion of the computer readable code; performing an initial determination to determine whether the CRC of the first portion of the computer readable code is present in a database of CRCs, each CRC including corresponding instructions for how to proceed if the determined CRC is present in the database of CRCs; and if it is determined that the CRC of the first portion of the computer readable code is present in the database of CRCs, performing the corresponding instructions.

30. A programmed computer apparatus as recited in claim 29, wherein the corresponding instructions comprise at least one of directing that a CRC of the entire computer readable code be determined and compared with the database of CRCs, directing that a CRC of a constant portion of the computer readable code be determined and compared with the database of CRCs, directing that a form of malicious code detection other than CRC checks be performed on the computer readable code.

Description

REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims the benefit of Provisional Application Serial No. 60/372,283 filed Apr. 13, 2002 and Provisional Application Serial No. 60/372,473 filed Apr. 15, 2002, the entire contents of both of which are herein incorporated by reference.

BACKGROUND OF THE DISCLOSURE

[0002] 1. Field of the Disclosure

[0003] The present disclosure relates to a system and method for detecting malicious code.

[0004] 2. Description of the Related Art

[0005] Each year, more and more computer viruses and variations of computer viruses are encountered. The required effort to maintain computer systems free from such viruses has increased dramatically. One